

THE PRIME-TO- p PART OF ÉTALE FUNDAMENTAL GROUPS OF CURVES

HILAF HASSON

ABSTRACT. Let K be a strictly henselian field of mixed characteristic $(0, p)$. We describe explicitly the action of the absolute Galois group of K on the prime-to- p étale fundamental group of the projective line \mathbb{P}_K^1 minus finitely many points. This allows us to compute prime-to- p étale fundamental groups over strictly henselian fields. For example, for $p \neq 2$ we give an explicit presentation of the prime-to- p fundamental group of the complement of $\{0, p^m, 1, 2\}$ in the projective line over \mathbb{Q}_p^{un} . We explore global and local applications of this result to the ramification of primes in the field of moduli of branched Galois covers.

1. OVERVIEW

Let K be the quotient field of a strictly henselian DVR R , of characteristic 0, residue characteristic $p \geq 0$ and uniformizing parameter t . (For example, $K = \mathbb{Q}_p^{\text{un}}$ or $\mathbb{C}((t))$.) Let a_1, \dots, a_r be closed points of \mathbb{P}_K^1 whose images in \mathbb{P}_K^1 have residue field K . The main theorem of this paper (Theorem 3.1) describes the action of $\text{Gal}(K)$ on the prime-to- p étale fundamental group $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\})$ in terms of topological fundamental groups. As a consequence of this result, we describe the prime-to- p étale fundamental group $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\})$ (see Section 7).

Every G -Galois branched cover of $\mathbb{P}_{\mathbb{Q}}^1$ has an associated field called the “field of moduli”, and it is equal to the intersection of all of its fields of definition (see [4]). Sybilla Beckmann ([2]) gave a condition, based on topological data, for rational primes that don’t divide $|G|$ to be unramified in the field of moduli. Stéphane Flon ([6]) has strengthened her result, and gave an “if and only if” condition for primes not dividing $|G|$ to be unramified in the field of moduli. Stefan Wewers ([17]) and Andrew Obus ([11] and [12]), on the other hand, have explored the ramification of primes that do divide $|G|$ (in the case that the cover ramifies over at most 3 points).

In this context, the main result of this paper (Theorem 3.1) helps to explain the phenomenon of the ramification of primes that don’t divide $|G|$ in the field of moduli in terms of étale fundamental groups. (See Section 8 for more about how to relate Theorem 3.1 with G -Galois covers defined over $\bar{\mathbb{Q}}$.) The main result also shares similar themes with Jakob Stix’s work ([14]). Furthermore, in Section 5, I simplify (in the language of étale fundamental groups) Flon’s condition for the ramification of primes in the field of moduli, which allows me to prove Corollary 5.3 about the index of ramification of primes in the field of moduli. The main theorems of Section 9 (Theorems 9.1 and 9.6) show that by choosing the branch points carefully, we can guarantee that many primes will be unramified in the field of moduli simultaneously.

This result is closely related to the Regular Inverse Galois Problem. The problem asks whether for every finite group G there is a G -Galois branched cover of the projective line that is defined over \mathbb{Q} . If the answer is positive, then by Hilbert’s Irreducibility Theorem ([7], Chapter 11) so is the answer to the Inverse Galois Problem. It is well known that every finite group G appears as a principal G -bundle of the Riemann Sphere minus finitely many algebraic points. By Riemann’s Existence Theorem ([9]), every such principal G -bundle can be cut out by polynomials with coefficients in a number field. Much of the work towards the Inverse Galois Problem has involved understanding the mysterious connection between the coefficients of these polynomial and topological data.

The outline of the paper is as follows. Section 2 will present the notations and definitions that will be used in the paper. Section 3 states the main theorem of this paper. In Section 4 we give a proof of a slightly weaker version (Proposition 4.1) of Theorem 3.1, and in Section 6 we finish the proof. Section 5 provides an algorithm for explicit computations. Section 7 shows how to use Theorem 3.1 to compute the prime-to- p étale fundamental group of $\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}$, and provides examples. Section 8 provides a way to relate the ramification of primes in the field of moduli of covers of $\mathbb{P}_{\mathbb{Q}}^1$ with that of covers of the projective line over p -adic fields. Section 9 gives applications of all of the above to the study of the ramification of primes in the field of moduli in the sense of Beckmann ([2]). Finally, in Section 10, I present a new theorem (Theorem 10.2), inspired by the philosophy of Theorem 3.1, generalizing a result of Beckmann's (Theorem 10.1) about vertical ramification.

This paper was largely based on the author's doctoral thesis, written at the University of Pennsylvania under the supervision of David Harbater. The author would like to thank Andrew Obus and Florian Pop for helpful discussions concerning material related to this paper.

2. DEFINITIONS

Notation 2.1. Let G be a group, and let g and h be elements of G . We will use the notation g^h to mean $h^{-1}gh$, and the notation ${}^h g$ to mean hgh^{-1} .

Notation 2.2. Given an integral scheme S , we write $\kappa(S)$ for its function field. (I.e. its stalk at the generic point.)

Definition 2.3. We say that a map $X \rightarrow Y$ of integral schemes is called a *branched cover* (or simply a *cover*) if it is finite and generically étale. We say that a branched cover is *Galois* if it is connected, and the induced extension on function fields $\kappa(X)/\kappa(Y)$ is a Galois extension of fields. We sometimes refer to branched covers as *mere covers*.

Let G be a finite group. A G -Galois branched cover is a branched cover $X \rightarrow Y$ which is Galois, together with an isomorphism of $\text{Gal}(\kappa(X)/\kappa(Y))$ with G .

Definition 2.4. Let $X_L \rightarrow Y_L$ be a (resp. G -Galois) branched cover of varieties over a field L . Let K be a subfield of L . The field of moduli of $X_L \rightarrow Y_L$ as a mere cover (resp. a G -Galois cover) relative to K is the subfield of \bar{L} fixed by those automorphisms of $\text{Gal}(\bar{L}/K)$ that take the mere cover (resp. G -Galois cover) to an isomorphic copy of itself.

We say that $K \subset L$ is a field of definition of a G -Galois branched cover (resp. mere cover) $X_L \rightarrow Y_L$ of varieties over L if there is a G -Galois branched cover (resp. mere cover) $X_K \rightarrow Y_K$ such that $X_L \rightarrow Y_L$ is its base change to L .

Remark 2.5.

- (1) Even though “field of moduli” is a relative term, we will use the convention that (unless otherwise stated) the field of moduli of a (resp. G -Galois) branched cover of varieties over \mathbb{Q} would mean the field of moduli relative to \mathbb{Q} .
- (2) Given a G -Galois branched covering, the term “field of moduli” will refer to “field of moduli as a G -Galois branched covering” unless otherwise stated.
- (3) Note that the field of moduli of a G -Galois branched covering (resp. mere covering) of curves over a field L is contained in every field of definition (resp. field of definition as a mere covering).

Definition 2.6. Let G be a group. We denote by \hat{G} its profinite completion. I.e. $\hat{G} = \varprojlim G/N$ as N runs over the normal subgroups of G of finite index.

Let G be a profinite group, and p be a prime. We denote by $G^{(p')}$ its maximal prime-to- p quotient. I.e. $G^{(p')} = \varprojlim G/N$ as N runs over the open normal subgroups of G whose index is a finite prime-to- p number. By convention $G^{(0')}$ would simply mean G .

Definition 2.7. Given a scheme S and a geometric point \bar{o} , let $\text{Fib}_{\bar{o}}$ be the functor from the category of finite étale covers of S to the category of sets that takes a cover to the geometric fiber of it over \bar{o} . Denote by $\pi_1(S, \bar{o})$ the automorphism group of $\text{Fib}_{\bar{o}}$. We say that $\pi_1(S, \bar{o})$ is the étale fundamental group of S with basepoint \bar{o} .

Let p be a prime number. Where it does not lead to confusion, we will denote by $\pi_1'(S, \bar{o})$ the profinite group $\pi_1(S, \bar{o})^{(p')}$. We say that $\pi_1'(S, \bar{o})$ is the prime-to- p fundamental group of S with basepoint \bar{o} .

For a topological space X , and a point $x \in X$, we denote by $\pi_1^{\text{top}}(X, x)$ the topological fundamental group of X with basepoint x .

Notation 2.8. Let $X_{\mathbb{C}}$ be a complex variety. We denote by $(X_{\mathbb{C}})^{\text{an}}$ the set $X_{\mathbb{C}}(\mathbb{C})$ together with the analytic topology.

Let a_1, \dots, a_r be points of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$. For every i let B_i be a small open ball around a_i such that $B_i \cap B_j = \emptyset$ for $i \neq j$. Let c_i be some point in B_i different from a_i , and let γ_i be a loop in $B_i \setminus \{a_i\}$, beginning and ending at c_i , that goes around a_i once in a counter-clockwise fashion.

Let u be a point in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \cup_i B_i$. Let $\mathbb{A}_{\mathbb{C}}^1$ be an affine patch of $\mathbb{P}_{\mathbb{C}}^1$ centered at u , and let B be a ball with radius R centered at u that doesn't intersect any of the B_i 's. For every $i = 1, \dots, r$ and $0 \leq t \leq 1$ define $\eta_i(t) = Rte^{\frac{2\pi\sqrt{-1}}{i}}$ (in the coordinates of $\mathbb{A}_{\mathbb{C}}^1$).

Definition 2.9. Elements $\alpha_1, \dots, \alpha_r \in \pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)$ are called a bouquet of loops around a_1, \dots, a_r if there are simple paths ϵ_i from $\eta_i(1)$ to c_i , whose pairwise intersections are trivial, such that α_i is represented by $\eta_i \epsilon_i \gamma_i \epsilon_i^{-1} \eta_i^{-1}$ for $i = 1, \dots, r$.

Note that if $\alpha_1, \dots, \alpha_r$ are a bouquet of loops then

$$\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u) \cong \langle \alpha_1, \dots, \alpha_r \mid \alpha_1 \cdots \alpha_r = 1 \rangle.$$

Definition 2.10. Let $\underline{a} = (a_1, \dots, a_r)$ be an r -tuple of distinct points on the Riemann Sphere $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$. We say that two homeomorphisms D_1 and D_2 from $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ to itself that fix \underline{a} are \underline{a} -isotopic if there exists a homotopy $H : (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \times [0, 1] \rightarrow (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that for every $t \in [0, 1]$ the map $H(_, t) : (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \rightarrow (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ is a homeomorphism that fixes \underline{a} .

Definition 2.11. Fix a tuple $\underline{a} = (a_1, \dots, a_r)$ of distinct points on the Riemann sphere $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$. We denote by $\Gamma_{0,r}$ the group of homeomorphisms, up to \underline{a} -isotopies, from $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ to itself that fix \underline{a} . We say that $\Gamma_{0,r}$ is the Mapping Class Group of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ with marks \underline{a} .

Let $(U_{\mathbb{C}}^r)^{\text{an}}$ be $((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}})^r \setminus \Delta$, where Δ is the weak diagonal. (This jibes with the definition of $(U_{\mathbb{C}}^r)^{\text{an}}$ in Section 4.3.) Fix a tuple $\underline{a} = (a_1, \dots, a_r)$ of distinct points on the Riemann sphere $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$. For every $b \in \pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a})$, there exists a homotopy $H : (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \times [0, 1] \rightarrow (\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ of homeomorphisms (that don't necessarily fix \underline{a}) such that $H(_, 0)$ is the identity, and $H(a_i, t)$ is equal to the i^{th} projection of $b(t)$ to $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$. There is a natural homomorphism $\phi : \pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a}) \rightarrow \Gamma_{0,r}$ taking b to $[H(_, 1)]$. The following theorem is well known ([3]).

Theorem 2.12. The homomorphism ϕ above is surjective, with kernel the center of $\pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a})$. Furthermore, the center of $\pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a})$ is of order 2.

Let u be some point of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ different from a_1, \dots, a_r . Then the group $\pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a})$ acts on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)$ by monodromy. Let this action be denoted by

$$\delta_1 : \pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, \underline{a}) \rightarrow \text{Aut}(\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)).$$

Claim 2.13. *There exists an action of the mapping class group $\Gamma_{0,r}$ with respect to \underline{a} on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)$ given by*

$$\delta_2 : \Gamma_{0,r} \rightarrow \text{Aut}(\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u))$$

such that $\delta_2 \circ \phi = \delta_1$.

Dehn twists are specific elements in the Mapping Class Group of particular importance. See [5] for more details. We will use the convention that a Dehn twist along a simple loop γ is made by twisting the inner rim of a tubular neighborhood of γ counterclockwise.

3. MAIN THEOREM

Let K be the quotient field of a strictly henselian DVR R , of characteristic 0, residue characteristic $p \geq 0$ and uniformizing parameter t . Let a_1, \dots, a_r be K -rational points on \mathbb{P}_K^1 , and fix a geometric base point \bar{o} over a K -rational point of $\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}$.

The base point induces an action of $\text{Gal}(K)$ on every Galois cover of \mathbb{P}_K^1 ramified only over a_1, \dots, a_r , and so in particular on the prime-to- p étale fundamental group $\pi_1'(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$.

We may think of $\text{Spec}(R)$ as an infinitesimally small disc and of $\text{Spec}(K)$ as an infinitesimally small punctured disc. Theorem 3.1 asserts that the $\text{Gal}(K)$ action on $\pi_1'(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ agrees with this intuition; namely that this action is “the same” as the monodromy action of $\mathcal{T} \rightarrow B \setminus \{0\}$, where B is a small disc, and \mathcal{T} is a family of projective lines with certain sections removed.

To say this more precisely, we introduce the following notation. Let e_{ij} be the intersection number between a_i and a_j in the scheme \mathbb{P}_R^1 . Let $b_1(x), \dots, b_r(x) \in \mathbb{C}[x]$ be polynomials such that $v_x(b_i(x) - b_j(x)) = e_{ij}$, and let B be a small open ball around 0 in \mathbb{C} of radius ϵ . Finally, let $\mathcal{T} := ((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \times (B \setminus \{0\})) \setminus \{(b_i(x), x) | x \in B \setminus \{0\}\}_i$. Choosing some point c in $B \setminus \{0\}$, and a base point u in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$, induces a monodromy action of $\hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)$ on every Galois cover of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ ramified only over $b_1(c), \dots, b_r(c)$; and so in particular on $\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}$ (recall that the superscript (p') denotes the maximal prime-to- p quotient of a group). Let \mathcal{D} be the image in $\hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)$ of a loop going once around the origin in a counter-clockwise fashion.

Theorem 3.1. *In the situation above, the following holds:*

- (1) *The action of $\text{Gal}(K)$ on $\pi_1'(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ factors through $\text{Gal}(K)^{(p')}$.*

Furthermore, there exists a sufficiently small $\epsilon > 0$ such that:

- (2) *The action of $\hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)$ on $\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}$ factors through $\hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')}$.*
- (3) *There exist isomorphisms ϕ_1 and ϕ_2 such that the following commutes:*

$$\begin{array}{ccc} \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')} & \xrightarrow{\rho_1} & \text{Aut}(\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}) \\ \downarrow \phi_1 & & \downarrow \phi_2 \\ \text{Gal}(K)^{(p')} & \xrightarrow{\rho_2} & \text{Aut}(\pi_1'(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})) \end{array}$$

Theorem 3.1 will allow us in turn to give an explicit description to the prime-to- p étale fundamental groups of \mathbb{P}_K^1 minus finitely many K -rational points. See Section 7 for examples.

4. PROOF OF MAIN THEOREM

In the remainder of this section we prove a weaker, less symmetric, version of Theorem 3.1 (Proposition 4.1 below). We postpone the proof of Theorem 3.1 to Section 6.

Proposition 4.1. *In the situation of Theorem 3.1, the following hold:*

- (1) *The action of $\text{Gal}(K)$ on $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ factors through $\text{Gal}(K)^{(p')}$.*
- (2) *There exists a sufficiently small $\epsilon > 0$ such that there exist an epimorphism ϕ'_1 and an isomorphism ϕ_2 that make the following diagram commute:*

$$\begin{array}{ccc} \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c) & \xrightarrow{\rho'_1} & \text{Aut}(\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}) \\ \downarrow \phi'_1 & & \downarrow \phi_2 \\ \text{Gal}(K)^{(p')} & \xrightarrow{\rho_2} & \text{Aut}(\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})) \end{array}$$

The proof is heavily influenced by the work of Stéphane Flon ([6]) on ramification of primes in the field of moduli. The proof will proceed through the following steps:

- (1) Description of the topological action via Dehn twists.
- (2) Reduction to the case that $|K| = \aleph_0$.
- (3) Arithmetic action via moduli spaces.
- (4) Description of the arithmetic action via Dehn twists.

4.1. Description of the Topological Action via Dehn Twists. In order to state Theorem 4.5 below describing the topological action, we require the terminology of stable marked curves.

Definition 4.2. *Let R be a strictly henselian DVR, let Y_R be a relative curve over R , and let D_R be a divisor on Y_R . Then (Y_R, D_R) is said to be a stable marked curve if the following hold:*

- (1) *The scheme Y_R is reduced.*
- (2) *The curve $Y_{\text{Quot}(R)}$ is smooth and geometrically irreducible.*
- (3) *The special fiber of Y_R has only nodes as singularities.*
- (4) *The natural map $D_R \rightarrow \text{Spec}(R)$ is étale, and D_R intersects the special fiber at smooth points.*
- (5) *For every genus 0 component in the special fiber of Y_R , the sum of the number of its intersections with other components plus the number of its intersections with D_R is at least 3.*

Definition 4.3. *Let R be a strictly henselian DVR with fraction field K , and let D_R be a divisor of \mathbb{P}_R^1 made up of a formal sum of closed points that have residue field K . Then there is a unique choice of a relative curve Y_R over R , a divisor \mathfrak{D}_R on Y_R , and a map $Y_R \rightarrow \mathbb{P}_R^1$ made up consecutive blow ups at closed points, such that (Y_R, \mathfrak{D}_R) is a stable marked curve, and such that \mathfrak{D}_R maps to D_R . We say that (Y_R, \mathfrak{D}_R) is the stable marked reduction of (\mathbb{P}_R^1, D_R) . We call the strict transform of the special fiber of \mathbb{P}_R^1 in Y_R the original component.*

Definition 4.4. *Let R be a strictly henselian DVR with parametrizing element t , let X_R be a normal relative curve over R , and let x be an ordinary double point on its special fiber. The thickness of x is the natural number n such that X_R formally locally at x is isomorphic to $\text{Spec}(R[[x, y]]/xy - t^n)$.*

In the situation of Theorem 3.1, blow up $\mathbb{P}_{\mathbb{C}[[x]]}^1$ with marks $b_1(x), \dots, b_r(x)$ to get a stable marked curve \hat{X} (see Definitions 4.2 and 4.3). Let X be the closed fiber of \hat{X} . For every node v , let $I_v \subset \{1, \dots, r\}$ be the set of indices such that $b_i(x)$ does not intersect the connected component of

the original component (see Definition 4.3) in $X \setminus \{v\}$. Let C_v be a choice of a simple loop in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that one connected component of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus C_v$ contains $\{b_i(c) | i \in I_v\}$, and the other contains $\{b_i(c) | i \notin I_v\}$. I further require that the C_v 's are chosen so that C_v does not intersect C_w for $v \neq w$. Let θ_v be the thickness of the node v in \hat{X} . (See Definition 4.4.)

Finally let \mathcal{D} be the loop in $\pi_1^{\text{top}}(B \setminus \{0\}, c)$ given by $e^{t\sqrt{-1}}c$ as t goes from 0 to 2π .

Theorem 4.5. *In the situation above, we can choose $\epsilon > 0$ (the radius of B) to be small enough so that the action of \mathcal{D} on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$ is equal to the action of $\prod D_v^{\theta_v}$ on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$, where D_v is the Dehn twist along C_v .*

In order to prove this theorem, we will require two lemmas.

Lemma 4.6. *In the situation above, for every $\epsilon' > 0$ there exists an $\epsilon > 0$ such that for every $i = 1, \dots, r$ we have $\sup_{x \in B_{\epsilon}(0)} (|b_i(x) - b_i(0)|) \leq \epsilon'$.*

Proof. This follows immediately from the continuity of the map from \mathbb{C} to \mathbb{C}^r given by $x \mapsto (b_1(x), \dots, b_r(x))$. \square

In order to simplify notation, make the following extra assumption.

Hypotheses 4.7. *Assume that for every m the function taking values in $\{m+1, \dots, r\}$ defined by $l \mapsto e_{ml}$ (the intersection number of $b_m(x)$ with $b_l(x)$) is monotonically decreasing in the weak sense.*

This can always be done by reordering the $b_i(x)$'s.

In the situation above, let k be some complex number. Let

$$\{b_j(x) \text{ s.t. } x \text{ divides } b_j(x) - k, \text{ and s.t. } j \in \{1, \dots, r\}\} = \{b_i(x), \dots, b_{i+l}(x)\},$$

i.e., $b_j(x) - k = xg_j(x)$ for every $j = i, \dots, i+l$. (The indices of the b_i 's in this set are consecutive because of Hypotheses 4.7.) Let C_{sep} be a simple loop in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that one of the connected components of its complement contains $\{b_i(c), \dots, b_{i+l}(c)\}$, and the other contains $\{b_1(c), \dots, b_{i-1}(c), b_{i+l+1}(c), \dots, b_r(c)\}$. In the lemma below we construct a homotopy between two loops in $(U^r)^{\text{an}}$. Lemma 4.6 will help us prove that this homotopy is well defined.

Lemma 4.8. *In the situation above, we may choose the ball B to be small enough so that the braid given by the loop*

$$(b_1(ce^{\sqrt{-1}t}), \dots, b_r(ce^{\sqrt{-1}t}))_{0 \leq t \leq 2\pi}$$

in $\pi_1^{\text{top}}((U_{\mathbb{C}}^r)^{\text{an}}, (b_1(c), \dots, b_r(c)))$ is homotopic to the concatenation of

$$(b_1(c), \dots, b_{i-1}(c), k + ce^{\sqrt{-1}t}g_i(c), \dots, k + ce^{\sqrt{-1}t}g_{i+l}(c), b_{i+l+1}(c), \dots, b_r(c))_{0 \leq t \leq 2\pi}$$

with

$$(b_1(ce^{\sqrt{-1}t}), \dots, b_{i-1}(ce^{\sqrt{-1}t}), k + cg_i(ce^{\sqrt{-1}t}), \dots, k + cg_{i+l}(ce^{\sqrt{-1}t}), b_{i+l+1}(ce^{\sqrt{-1}t}), \dots, b_r(ce^{\sqrt{-1}t}))_{0 \leq t \leq 2\pi}.$$

Proof. We may define the homotopy $H(A, t)$, where $0 \leq A \leq 1$, thusly.

For $0 \leq t \leq \frac{A}{2}$:

$$\begin{aligned} H(A, t) = & (b_1(c), \dots, b_{i-1}(c), \\ & k + cg_i(ce^{\frac{2}{2-A}t\sqrt{-1}}), \dots, k + cg_{i+l}(ce^{\frac{2}{2-A}t\sqrt{-1}}), \\ & b_{i+l+1}(c), \dots, b_r(c)) \end{aligned}$$

For $\frac{A}{2} \leq t \leq \frac{2-A}{2}$:

$$H(A, t) = (b_1(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \dots, b_{i-1}(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \\ k + ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}g_i(ce^{\frac{2}{2-A}t\sqrt{-1}}), \dots, k + ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}g_{i+l}(ce^{\frac{2}{2-A}t\sqrt{-1}}), \\ b_{i+l+1}(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \dots, b_r(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}))$$

For $\frac{2-A}{2} \leq t \leq 1$:

$$H(A, t) = (b_1(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \dots, b_{i-1}(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \\ k + ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}g_i(c), \dots, k + ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}g_{i+l}(c), \\ b_{i+l+1}(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}), \dots, b_r(ce^{\frac{2}{2-A}(t-\frac{A}{2})\sqrt{-1}}))$$

It remains to show that for every A and t , the point $H(A, t)$ is in $(U^r)^{\text{an}}$, i.e. that the coordinates of $H(A, t)$ are different from one another. Since $b_1(x), \dots, b_r(x)$ are polynomials, we may choose B to be small enough so that $b_i(x) \neq b_j(x)$ for every $x \in B \setminus \{0\}$. This implies that for every A and t , any two coordinates in $\{i, \dots, i+l\}$ are different from one another, and any two coordinates in $\{1, \dots, i-1, i+l+1, \dots, r\}$ are different from one another. Lemma 4.6 for a sufficiently small ϵ' (for example $\epsilon' = \frac{1}{3} \min_{b_i(0) \neq b_j(0)} (b_i(0) - b_j(0))$) ensures that we may choose B small enough so that the supremum of the distances between k and $b_j(x)$ as j goes over $i, \dots, i+l$ and x goes over B is smaller than the infimum of the distances between k and $b_j(x)$ as j goes over $1, \dots, i-1, i+l+1, \dots, r$ and x goes over B . Fix j to be some natural number between i and $i+l$. Note that for $0 \leq t \leq \frac{A}{2}$ the distance of the j^{th} coordinate from k is equal to the distance of $b_j(ce^{\frac{2}{2-A}t\sqrt{-1}})$ from k ; for $\frac{A}{2} \leq t \leq \frac{2-A}{2}$ the distance of the j^{th} coordinate from k is equal to the distance of $b_j(ce^{\frac{2}{2-A}t\sqrt{-1}})$ from k ; and for $\frac{2-A}{2} \leq t \leq 1$ the distance of the j^{th} coordinate from k is equal to the distance of $b_i(c)$ from k . Therefore, by the above, this implies that for those values of A and t the j^{th} coordinate is different from the coordinates in $\{1, \dots, i-1, i+l+1, \dots, r\}$, and therefore the point $H(A, t)$ lies in $(U^r)^{\text{an}}$. Since we have covered all values of A and t , this concludes the proof. \square

Remark 4.9. In the situation above, let C_{sep} be a simple loop in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that one of the connected components of its complement contains $\{b_i(c), \dots, b_{i+l}(c)\}$, and the other contains $\{b_1(c), \dots, b_{i-1}(c), b_{i+l+1}(c), \dots, b_r(c)\}$. Then the first loop in the concatenation mentioned in Lemma 4.8 maps to the Dehn twist along C_{sep} in the Mapping Class Group $\Gamma_{0,r}$ (see Definition 2.11).

We are now ready to prove Theorem 4.5.

Proof. (of Theorem 4.5)

We will prove Theorem 4.5 by induction on the sum of the thicknesses $\sum_v \theta_v$ in \hat{X} .

If $\sum_v \theta_v = 0$, then Theorem 4.5 is trivial. Otherwise, there is a complex number k such that $\{b_j(x) \text{ s.t. } x \text{ divides } b_j(x) - k, \text{ and s.t. } j \in \{1, \dots, r\}\}$ is nonempty. Let

$$\{b_j(x) \text{ s.t. } x \text{ divides } b_j(x) - k, \text{ and s.t. } j \in \{1, \dots, r\}\} = \{b_i(x), \dots, b_{i+l}(x)\},$$

i.e. $b_j(x) - k = xg_j(x)$. Let w be the node in X described by $x = k$ on the original component. Since the sum of the thicknesses of the stable marked reduction of $\mathbb{P}_{\mathbb{C}[[x]]}^1$ with marks $b_1(x), \dots, b_{i-1}(x), k + cg_i(x), \dots, k + cg_{i+l}(x), b_{i+l+1}(x), \dots, b_r(x)$ is smaller than $\sum_v \theta_v$, we may use Theorem 4.5 for these polynomials as the inductive step. By Lemma 4.8, together with Remark 4.9, we see that the action of the braid $(b_1(ce^{\sqrt{-1}t}), \dots, b_r(ce^{\sqrt{-1}t}))_{0 \leq t \leq 2\pi}$ on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$, which is identical to the action of \mathcal{D} , is equal to the action of D_w , followed by the action of the braid

$(b_1(ce^{\sqrt{-1}t}), \dots, b_{i-1}(ce^{\sqrt{-1}t}), k+cg_i(ce^{\sqrt{-1}t}), \dots, k+cg_{i+l}(ce^{\sqrt{-1}t}), b_{i+l+1}(ce^{\sqrt{-1}t}), \dots, b_r(ce^{\sqrt{-1}t}))_{0 \leq t \leq 2\pi}$. It is easy to see that Theorem 4.5 applied to the polynomials $b_1(x), \dots, b_{i-1}(x), k+cg_i(x), \dots, k+cg_{i+l}(x), b_{i+l+1}(x), \dots, b_r(x)$ proves that the action of this latter braid is equal to $D_w^{\theta_w-1} \prod_{v \neq w} D_v^{\theta_v}$. Therefore the action of \mathcal{D} on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$ is equal to the action of $\prod_v D_v^{\theta_v}$. \square

4.2. Reduction to the Case $|K| = \aleph_0$.

Lemma 4.10. *In the situation of Theorem 3.1, let E be the field of rationality of the image of the points a_1, \dots, a_r in $\mathbb{P}_{\mathbb{Q}}^1$. Then there exists a field L such that $E \subset L \subset K$, the field L is a strictly henselian field with parameter t , and $|L| = \aleph_0$.*

Proof. Let S' be $R \cap E(t)$. Let S be the integral closure of S' in K . Since R is integrally closed, it follows that S is a subring of R . Let $\mathfrak{p} \in \text{Spec}(S)$ be the intersection of tR and S . Note that \mathfrak{p} is a divisor of $\text{Spec}(S)$, and that since $\text{Spec}(S)$ is normal the localization $S_{\mathfrak{p}}$ is a DVR. Let Z be the maximal unramified algebraic extension of $S_{\mathfrak{p}}$ in K . It is clear that Z is a strictly henselian DVR, with parameter t (since t is in S). Finally, let $L = \text{Quot}(Z)$. It is clear from the construction that $|L| \leq \aleph_0$. Since L contains \mathbb{Q} , we have $|L| \geq \aleph_0$. Therefore $|L| = \aleph_0$. \square

In the situation of Lemma 4.10, we have the following commutative diagram:

$$\begin{array}{ccccccc}
 1 & \rightarrow & \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) & \xrightarrow{f_1} & \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) & \xrightarrow{g_1} & \text{Gal}(K)^{(p')} \rightarrow 1 \\
 & & \gamma_1 \downarrow & & \gamma_2 \downarrow & & \gamma_3 \downarrow \\
 1 & \rightarrow & \pi'_1(\mathbb{P}_L^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) & \xrightarrow{f_2} & \pi'_1(\mathbb{P}_L^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) & \xrightarrow{g_2} & \text{Gal}(L)^{(p')} \rightarrow 1
 \end{array}$$

Lemma 4.11. *In the diagram above, γ_1 , γ_2 and γ_3 are isomorphisms.*

Proof. That γ_1 and γ_3 are isomorphisms is obvious. The homomorphism γ_2 is an isomorphism by the Five Lemma. \square

If we choose our basepoint \bar{o} so that it would lie over an L -rational point in \mathbb{P}_L^1 , then this induces sections $s_1 : \text{Gal}(L)^{(p')} \rightarrow \pi'_1(\mathbb{P}_L^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ and $s_2 : \text{Gal}(K)^{(p')} \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$. Since these morphisms are induced by applying the prime-to- p étale fundamental group functor π'_1 on morphisms of schemes, it follows that s_1 and s_2 commute with the diagram above. This implies that it suffices to describe the action of $\text{Gal}(L)^{(p')}$ on $\pi'_1(\mathbb{P}_L^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$.

4.3. Arithmetic Action via Moduli Spaces. Assume the situation of Theorem 3.1. There exists a coarse moduli space H^r of pointed G -Galois covers of the projective line ramified over r points. This moduli space is called the Hurwitz moduli space. There also exists a fine moduli space U^r of r ordered points on the projective line. These moduli spaces are defined over \mathbb{Z} ([16], [8]). In [16], Stefan Wewers has shown that the natural map $\pi : H^r \rightarrow U^r$ is étale over \mathbb{Z} , and finite over $\mathbb{Z}[\frac{1}{|G|}]$. Furthermore, Wewers has constructed compactifications \bar{H}^r and \bar{U}^r such that this morphism extends $\bar{\pi} : \bar{H}^r \rightarrow \bar{U}^r$, and such that over $\mathbb{Z}[\frac{1}{|G|}]$ this morphism is finite and tamely ramified over a strictly normal crossing divisor. From now on when I write H^r , U^r , \bar{H}^r and \bar{U}^r I will mean their base change to R . Therefore $\bar{\pi}$ is finite and tame.

We now proceed to interpret Theorem 3.1 in terms of these moduli spaces.

By Section 4.2, we may assume without loss of generality that $|K| = \aleph_0$. Fix an embedding of \bar{K} into \mathbb{C} . Let \bar{o} be some \mathbb{C} -point of $\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}$ lying over a K -rational point. The induced homomorphism $\pi'_1(\mathbb{P}_{\mathbb{C}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \pi'_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ is an isomorphism (Lefschetz principle).

By Riemann's Existence Theorem ([9]) $\pi'_1(\mathbb{P}_{\mathbb{C}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ is isomorphic to the maximal prime-to- p quotient of the profinite completion of the corresponding topological fundamental group. We may, therefore, fix an isomorphism of $\pi'_1(\mathbb{P}_{\mathbb{C}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ with $\langle \alpha_1, \dots, \alpha_r | \widehat{\alpha_1 \dots \alpha_r} = 1 \rangle^{(p')}$. (At this point we allow any such isomorphism, although in Section 5 we will describe a specific isomorphism that is helpful in doing computations.)

We note that a pointed G -Galois étale cover over $\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}$ is equivalent to giving a surjection $\pi'_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \twoheadrightarrow G$. Such a surjection is fully determined by the images of the α_i 's above. I.e., it suffices to give an r -tuple of generators (g_1, \dots, g_r) of G such that $g_1 \cdots g_r = 1$. This r -tuple is called the branch cycle description of this cover, or simply its description.

The fundamental exact sequence

$$1 \rightarrow \pi_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \pi_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \text{Gal}(K) \rightarrow 1$$

splits via the underlying K -point of \bar{o} . This induces an action of $\text{Gal}(K)$ on $\pi_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ and in fact on $\pi'_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$.

Since $\pi'_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ is profinite, for every $\sigma \in \text{Gal}(K)$ the image of ${}^\sigma \alpha_1, \dots, {}^\sigma \alpha_r$ in all of its finite quotients determines the elements ${}^\sigma \alpha_1, \dots, {}^\sigma \alpha_r$. It suffices therefore to fix a prime-to- p group G and a surjection $\phi : \pi'_1(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \twoheadrightarrow G$, and to describe $\phi({}^\sigma \alpha_1), \dots, \phi({}^\sigma \alpha_r)$ in G .

In other words, it suffices to see how $\text{Gal}(K)$ acts on the set of G -Galois pointed covers of $\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}$. This is equivalent to the action of $\text{Gal}(K)$ on the points in $H^r(\bar{K})$ lying over the point in $U^r(\bar{K})$ corresponding to (a_1, \dots, a_r) .

4.4. Description of the Arithmetic Action via Dehn Twists. Assume the situation of Theorem 3.1. Let \bar{x} be an element of $H^r(\bar{K})$ lying over the point \bar{y} in $U^r(\bar{K})$ that corresponds to the set of points (a_1, \dots, a_r) . Since base change to \mathbb{C} gives a bijection between $H^r(\bar{K})$ and $H_{\mathbb{C}}^r(\mathbb{C})$, the element \bar{x} corresponds to a G -Galois pointed cover of $\mathbb{P}_{\mathbb{C}}^1$ ramified over the r points a_1, \dots, a_r .

Blow up $\mathbb{P}_{\mathbb{C}}^1$ with marks a_1, \dots, a_r to get a stable marked curve \hat{X} (see Definitions 4.2 and 4.3). Let X be the closed fiber of \hat{X} . Let W be the set of nodes of \hat{X} . For every node $v \in W$, let $I_v \subset \{1, \dots, r\}$ be the set of indices such that a_i does not intersect the connected component of the original $\mathbb{P}_{\mathbb{C}}^1$ in $X \setminus \{v\}$. Let C_v be a choice of a simple loop in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that one connected component of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus C_v$ contains $\{a_i | i \in I_v\}$, and the other contains $\{a_i | i \notin I_v\}$. I further require that the C_v 's are chosen so that C_v does not intersect C_w for $v \neq w$. Let θ_v be the thickness of the node v in \hat{X} . (See Definition 4.4.)

Let $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}}$ for every natural number m . Finally let δ be the element in $\text{Gal}^{\text{tame}}(K)$ that takes $t^{\frac{1}{m}}$ to $\zeta_m t^{\frac{1}{m}}$ for every m coprime to p .

Theorem 4.12. *In the situation above, the following hold:*

- (1) *The action of $\text{Gal}(K)$ on \bar{x} factors through the group $\text{Gal}^{\text{tame}}(K)$.*
- (2) *The action of δ on \bar{x} is equal to the action of $\prod_{v \in W} D_v^{\theta_v}$ on \bar{x} , where D_v is the Dehn twist along C_v . (Here the action of the Mapping Class Group of the set of G -Galois pointed covers ramified over a_1, \dots, a_r is defined via its action on $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\})$.)*

Remark 4.13. Theorem 4.12 above should be thought of as the arithmetic analog of Theorem 4.5.

In order to prove this theorem, we require several lemmas and claims.

Lemma 4.14. *Let R , K and δ be as in Theorem 4.12, and let l be a natural number between 1 and n . Let $s : \text{Spec}(R) \rightarrow \text{Spec}(R[[x_1, \dots, x_n]]^{\text{alg}})$ be a section whose generic point doesn't lie in $(x_1 \cdots x_l)$. For $i = 1, \dots, l$, let σ_i in $\pi_1^{\text{tame}}(R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}])$ be defined by $x_j^{\frac{1}{m}} \mapsto \zeta_m x_j^{\frac{1}{m}}$ for*

$j = i$, and $x_j^{\frac{1}{m}} \mapsto x_j^{\frac{1}{m}}$ for $j \neq i$. Let e_i be the intersection multiplicity of this section with x_i . Let $s' : \text{Spec}(K) \rightarrow \text{Spec}(R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}])$ be the morphism induced by s . Then the induced morphism on fundamental groups $f : \text{Gal}^{\text{tame}}(K) \rightarrow \pi_1^{\text{tame}}(\text{Spec}(R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}]))$ takes δ in $\text{Gal}^{\text{tame}}(K)$ to $\sigma_1^{e_1} \cdots \sigma_l^{e_l}$.

Remark 4.15.

- (1) In the above, the base point of $\text{Spec}(R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}])$ is assumed to be the one induced by the map s' together with the given embedding of K into \bar{K} .
- (2) In order to see that the σ_i 's make sense, recall that Abhyankar's Lemma (in the version appearing in [10]) says that any cover of $R[[x_1, \dots, x_n]]^{\text{alg}}$ which is tamely ramified with respect to $(x_1 \cdots x_l)$ is a quotient of a cover given by $R[[x_1^{\frac{1}{m_1}}, \dots, x_l^{\frac{1}{m_l}}, x_{l+1}, \dots, x_n]]^{\text{alg}}$.

Proof. Write $f(\delta)$ as $\sigma_1^{m_1} \cdots \sigma_l^{m_l}$. Let i be an integer between 1 and l . By definition, for every natural number N that is prime to p , the automorphism σ_i acts on $R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}, y_i]/(y_i^N - x_i)$ by mapping y_i to $\zeta_N y_i$. Therefore $f(\delta)$ acts on $R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}, y_i]/(y_i^N - x_i)$ by mapping y_i to $\zeta_N^{m_i} y_i$ for every N prime to p .

By assumption, for every $j = 1, \dots, n$ the section s maps the element x_j to $u_j t^{e_j}$, where t is a parameterizing element of R , and the u_j 's are units.

Pulling back the cover $R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}, y_i]/(y_i^N - x_i)$ of $R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}]$ to a cover of K we get:

$$R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}, y_i]/(y_i^N - x_i) \otimes_{R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}]} K \cong K[y_i]/(y_i^N - t^{e_i}).$$

Therefore $f(\delta)$ maps the element y_i in $R[[x_1, \dots, x_n]]^{\text{alg}}[\frac{1}{x_1 \cdots x_l}, y_i]/(y_i^N - x_i)$ to $\zeta_N^{e_i} y_i$. We conclude that for every N that is coprime to p , $\zeta_N^{e_i} = \zeta_N^{m_i}$. Thus $e_i = m_i$. \square

The irreducible components of $\bar{U}^r \setminus U^r$ are in correspondence with the subsets of $\{1, \dots, r\}$ of cardinality at least two, and they form a strict normal crossing divisor. (See [16], [6], [8].) Let S^I denote the irreducible divisor corresponding to $I \subset \{1, \dots, r\}$.

Note that \bar{y} factors through a K -rational point $\Delta : \text{Spec}(K) \rightarrow U^r$, by assumption. By the valuative criterion of properness, the morphism Δ factors through a unique morphism $\tilde{\Delta} : \text{Spec}(R) \rightarrow \bar{U}^r$.

Definition 4.16. In the situation above, removing a node v from \hat{X} breaks the special fiber X into two connected components. Let X_v denote the connected component of $X \setminus \{v\}$ that doesn't include the original component (see Definition 4.3). Let Σ' be a map from the set of nodes of \hat{X} to the power set of $\{1, \dots, r\}$ defined by

$$\Sigma'(v) = \{i \mid \text{the Zariski closure of } a_i \text{ in } \hat{X} \text{ intersects } X_v\}.$$

The following follows from Proposition 3.6 in [6]:

Proposition 4.17. In the above situation, let C be the curve in \bar{U}^r parametrized by the section $\tilde{\Delta} : \text{Spec}(R) \rightarrow \bar{U}^r$. Then C intersects S^I if and only if I is in the image of Σ . Furthermore, the intersection multiplicity of C with S^I is equal to the thickness of the node $\Sigma^{-1}(I)$ in X (see Definition 4.4).

In particular, if we let T be the set of subsets $I \subset \{1, \dots, r\}$ such that the special point of $\tilde{\Delta}$ lies on S^I , then

$$T = \{I \subset \{1, \dots, r\} \mid \exists v \in W \text{ s.t. } I = I_v\}.$$

Let P be the image of the special point of $\mathrm{Spec}(R)$ under $\tilde{\Delta}$, and let $Q \in U^r(\mathbb{C})$ be the point induced by the generic point of $\mathrm{Spec}(R)$ via $\tilde{\Delta}$.

Let $\mathrm{Spec}(A) \subset \bar{U}^r$ be an open affine subset of \bar{U}^r about P , such that $\bar{U}^r \setminus U^r$ is given by the principal prime ideals $\cup_{I \in T} \{(x_I)\}$. Let $l = |T|$, and fix once and for all a bijection $\alpha : \{1, \dots, l\} \rightarrow T$. We write x_i to mean $x_{\alpha(i)}$. We may assume without loss of generality that x_1, \dots, x_l are a part of a regular system of parameters x_1, \dots, x_n at P .

Let $O_{\bar{U}^r, P}^{\mathrm{sh}}$ be the strict henselization of the local ring of X at P . Note that $(x_j)_{j \in T \cup J}$ give an isomorphism of $O_{\bar{U}^r, P}^{\mathrm{sh}}$ with $R[[x_1, \dots, x_n]]^{\mathrm{alg}}$. The section $\tilde{\Delta}$ factors through $\mathrm{Spec}(O_{\bar{U}^r, P}^{\mathrm{sh}})$ because the strict henselization of the stalk of \bar{U}^r at P is the stalk of \bar{U}^r at P in the étale topology. Furthermore, note that Δ factors through $\Phi : \mathrm{Spec}(K) \rightarrow \mathrm{Spec}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}])$.

Definition 4.18. *In the situation above, let Σ be defined as the composition $\alpha^{-1} \circ \Sigma'$.*

Lemma 4.19. *Let $\Sigma : W \rightarrow P(\{1, \dots, r\})$ be the map from Definition 4.18. For every $i = 1, \dots, l$ let $\sigma_i \in \pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}])$ be defined by $x_j^{\frac{1}{m}} \mapsto x_j^{\frac{1}{m}}$ and $x_i^{\frac{1}{m}} \mapsto e^{\frac{2\pi\sqrt{-1}}{m}} x_i^{\frac{1}{m}}$ for every m coprime to p and $j \neq i$. Then in the situation above, the homomorphism $\bar{\Phi} : \mathrm{Gal}^{\mathrm{tame}}(K) \rightarrow \pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}])$ takes δ to $\prod_{v \in W} \sigma_{\Sigma(v)}^{\theta_v}$.*

Proof. By Lemma 4.14, the element δ maps to $\prod_{v \in W} \sigma_{\Sigma(v)}^{e_v}$ where e_v is the intersection multiplicity of the image of the section $\tilde{\Delta}$ with $S^{\Sigma'(v)}$. By Proposition 4.17, we have that $e_v = \theta_v$. \square

Since $\bar{\pi} : \bar{H}^r \rightarrow \bar{U}^r$ is tame, the group $\pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}])$ acts on \bar{x} via the map $\pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}]) \rightarrow \pi_1^{\mathrm{tame}}(U^r, \bar{y})$. In [6], Flon argues that for every v the element $\sigma_{\Sigma(v)}$ in $\pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}])$ (defined as in Lemma 4.19) acts on \bar{x} in the same way the Dehn twist along C_v does. As his argument is difficult to read, I outline an alternative argument here.

Each \mathbb{C} -point C of A corresponds to a morphism of rings $g_C : A \rightarrow \mathbb{C}$. There exists an $\epsilon' > 0$ and a neighborhood N of $P \otimes \mathbb{C}$ in $\mathrm{Spec}(A)(\mathbb{C})$ such that the assignment $h : N \rightarrow B_{\epsilon'}(0)^n$ defined by $C \mapsto (g_C(x_j))_{j \in \{1, \dots, n\}}$ is a biholomorphism.

Let $N' = N \setminus \cup_{I \subset \{1, \dots, r\}, |I| \geq 2} S^I(\mathbb{C})$, and let Q' be a point in N' . Let V' be an open neighborhood in $(U^r)^{\mathrm{an}}$ that contains $N' \cup \{Q\}$, and that deformation retracts to N' . Let γ be any path in V' from Q to Q' . This γ gives an isomorphism $\pi_1^{\mathrm{top}}(V', Q) \cong \pi_1^{\mathrm{top}}(N', Q')$. It is easy to see that this isomorphism is independent of the choice of γ .

Lemma 4.20. *In the situation above, let the coordinates of $h(Q')$ be denoted by (Q'_1, \dots, Q'_n) . For every $i = 1, \dots, l$ let $\sigma'_i \in \hat{\pi}_1^{\mathrm{top}}(N', Q')^{(p')}$ be the element induced by the loop $h^{-1}(Q'_1, \dots, Q'_{i-1}, e^{2\pi\sqrt{-1}\theta} Q'_i, Q'_{i+1}, \dots, Q'_n)$, as θ goes from 0 to 2π . We will view σ'_i as an element of $\pi_1^{\mathrm{top}}(V', Q)^{(p')}$. For every $i = 1, \dots, l$ let $\sigma_i \in \pi_1^{\mathrm{tame}}(R[[x_1, \dots, x_n]]^{\mathrm{alg}}[\frac{1}{x_1 \cdots x_l}], Q)$ be defined by $x_j^{\frac{1}{m}} \mapsto x_j^{\frac{1}{m}}$ and $x_i^{\frac{1}{m}} \mapsto e^{\frac{2\pi\sqrt{-1}}{m}} x_i^{\frac{1}{m}}$ for every m coprime to p and $j \neq i$. We will view σ_i as an element in $\pi_1^{\mathrm{tame}}(O_{\bar{U}^r, P}^{\mathrm{sh}} \setminus (\cup S^I \times_{\bar{U}^r} O_{\bar{U}^r, P}^{\mathrm{sh}}), Q)$ via the natural isomorphism of $O_{\bar{U}^r, P}^{\mathrm{sh}}$ with $R[[x_1, \dots, x_n]]^{\mathrm{alg}}$. Then the action of σ'_i on \bar{x} is equal to the action of σ_i on \bar{x} for every $i = 1, \dots, l$.*

Proof. (sketch) There are global sections z_1, \dots, z_n of $\bar{H}^r \times_{\bar{U}^r} \mathrm{Spec}(A)$ that form a regular system of parameters at a point above P in the connected component of \bar{x} such that they are locally (in the analytic topology) the quotient of a cover Y defined by $y_i^m = x_i$ for every i . The point \bar{x} is the image of some point in Y with coordinates $y_i = \varOmega'_i$, where $\varOmega'_i{}^m = Q'_i$. It is clear that σ'_i acts on $(\varOmega'_1, \dots, \varOmega'_n)$ by taking it to $(\varOmega'_1, \dots, \varOmega'_{i-1}, e^{\frac{2\pi\sqrt{-1}}{m}} \varOmega'_i, \varOmega'_{i+1}, \dots, \varOmega'_n)$. It therefore agrees with the action of σ_i .

□

Claim 4.21. *For every $i = 1, \dots, l$, and $v \in W$, the element $\sigma_{\Sigma(v)}$ from Lemma 4.20 acts on \bar{x} in the same way the Dehn twist D_v along C_v does.*

Proof. Easy to verify using the construction of \bar{U}^r in [8]. (Where it is denoted B_r .) □

Claim 4.22 below phrases the action of δ on \bar{x} in terms of étale fundamental groups.

Claim 4.22. *Fix an algebraic closure \bar{K} of K . Let X and Y be connected schemes, and let $\pi : X \rightarrow Y$ be a finite étale map. Let $\bar{x} : \text{Spec}(\bar{K}) \rightarrow X$ be some \bar{K} -rational point of X lying over a K -rational point of Y , and let σ be an element of $\text{Gal}(\bar{K}/K)$. Then the geometric point given by composing \bar{x} with σ is equal to the geometric point given by the action of σ on $\bar{x} \in \text{Fib}_{\pi \circ \bar{x}}(X)$ via the natural map $\text{Gal}(\bar{K}/K) \cong \pi_1(\text{Spec}(K), \text{Spec}(\bar{K})) \rightarrow \pi_1(Y, \pi \circ \bar{x})$.*

In other words, the action of $\text{Gal}(K)$ on \bar{x} defined above is equal to the action induced by the map $\text{Gal}(K) \rightarrow \pi_1(U^r, \bar{y})$ (which is given by \bar{y}). The claim follows immediately from the definitions.

We are now ready to prove Theorem 4.12.

Proof. (Theorem 4.12)

Let $\Delta_* : \text{Gal}(K) \rightarrow \pi_1(U^r, \bar{y})$ be the map induced by Δ , and let $\bar{\Delta}$ be the composition of Δ_* with the quotient map $\pi_1(U^r, \bar{y}) \rightarrow \pi_1^{\text{tame}}(U^r, \bar{y})$. Let δ' be an element in $\text{Gal}(K)$ that maps to δ in $\text{Gal}^{\text{tame}}(K)$. By the functoriality of the tame fundamental group, the map $\bar{\Delta}$ factors through $\text{Gal}^{\text{tame}}(K)$. Since $\pi : H^r \rightarrow U^r$ is tame, this implies that the action of δ' on \bar{x} is independent of the choice of δ' . This proves the first claim in Theorem 4.12.

The map $\text{Gal}^{\text{tame}}(K) \rightarrow \pi_1^{\text{tame}}(U^r, \bar{y})$ induced by Δ factors through the map $\bar{\Phi} : \text{Gal}^{\text{tame}}(K) \rightarrow \pi_1^{\text{tame}}(R[[x_1, \dots, x_n]][\frac{1}{x_1 \cdots x_l}])$. By Lemma 4.19 we have $\bar{\Phi}(\delta) = \prod_{v \in W} \sigma_{\Sigma(v)}^{\theta_v}$, where Σ is as in Definition 4.18. By Lemma 4.20 together with Claim 4.21, we conclude that δ acts on \bar{x} in the same way $\prod_{v \in W} D_v^{\theta_v}$ does. □

4.5. Defining ϕ'_1 and ϕ_2 . We are now ready to prove Proposition 4.1.

Proof. Since $\text{Gal}^{\text{tame}}(K) = \text{Gal}(K)^{(p')}$, the first claim is equivalent to the first claim of Theorem 4.12 combined with Claim 4.22.

By Lemmas 4.10 and 4.11, we may assume without loss of generality that $|K| = \aleph_0$. This allows us to fix an embedding of \bar{K} into \mathbb{C} . Let \mathcal{D} be the counter-clockwise loop in $\pi_1^{\text{top}}(B \setminus \{0\}, c)$. Recall that $\delta \in \text{Gal}(K)^{(p')}$ denotes the element that takes $t^{\frac{1}{m}}$ to $e^{\frac{2\pi\sqrt{-1}}{m}} t^{\frac{1}{m}}$ for every m coprime to p . Let ϕ'_1 be the epimorphism taking the image of \mathcal{D} in $\hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')}$ to δ .

Let β_1, \dots, β_r be a bouquet of loops around a_1, \dots, a_r in $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, \bar{o})$. Let $\bar{\beta}_1, \dots, \bar{\beta}_r$ be their images in $\pi_1'(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$. Let $\alpha_1, \dots, \alpha_r$ be a bouquet of loops around $b_1(c), \dots, b_r(c)$ in $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$. Furthermore, let $\bar{\alpha}_1, \dots, \bar{\alpha}_r$ be the images of $\alpha_1, \dots, \alpha_r$ in $\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}$. Note that both $\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}$ and $\pi_1'(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ are isomorphic to the maximal prime-to- p quotient $\hat{F}_{r-1}^{(p')}$ of the free group on $r-1$ generators. Let ϕ_2 be the isomorphism induced by the isomorphism

$$\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')} \rightarrow \pi_1'(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$$

given by $\bar{\alpha}_j \mapsto \bar{\beta}_j$ for $j = 1, \dots, r$.

As the two descriptions of the actions (Theorem 4.5 for the geometric action, and Theorem 4.12 together with Section 4.2 for the arithmetic action) match for a small enough $\epsilon > 0$, we have that

$\phi_2 \circ \rho'_1(\mathcal{D}) = \rho_2 \circ \phi'_1(\mathcal{D})$. Since all of the morphisms are continuous, the diagram in Proposition 4.1 is commutative. Therefore the second claim of Proposition 4.1 holds. \square

We postpone the proof of Theorem 3.1 to Section 6.

5. ALGORITHM FOR EXPLICIT COMPUTATIONS

In Section 2.3 of [6], Flon gave an explicit description of the action of Dehn twists on a bouquet of loops $\alpha_1, \dots, \alpha_r \in \pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus r \text{ points})$. Thanks to Proposition 4.1, we may use his description to compute the action of $\text{Gal}(K)$ on $\pi_1'(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\})$ where a_1, \dots, a_r come from K -rational points on $\mathbb{P}_{\bar{K}}^1$. In this section we show that choosing a particular isomorphism of $\pi_1'(\mathbb{P}_{\bar{K}}^1 \setminus \{a_1, \dots, a_r\})$ with the maximal prime-to- p quotient of the profinite completion of $\langle \alpha_1, \dots, \alpha_r | \alpha_1 \cdots \alpha_r \rangle$ simplifies Flon's description considerably. In particular, this will allow us to get Corollary 5.3 regarding the index of ramification of primes in the field of moduli.

In the situation of Theorem 3.1, reorder the $b_i(x)$'s so that Hypotheses 4.7 will hold. Let $\alpha_1, \dots, \alpha_r$ be a bouquet of loops around $b_1(c), \dots, b_r(c)$ in $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$ (see Definition 2.9).

I will now proceed to explain how the generator $\mathcal{D} \in \pi_1(B \setminus \{0\}, c)$, defined by doing a counter-clockwise loop, acts on $\alpha_1, \dots, \alpha_r$. For simplicity, let's fix i and explain how \mathcal{D} acts on α_i . In order to do that, I require some notation.

Blow up $\mathbb{P}_{\mathbb{C}}^1[[x]]$ with marks $b_1(x), \dots, b_r(x)$ to get a stable marked curve \hat{X} (see Definitions 4.2 and 4.3). Let X be the closed fiber of \hat{X} . For every node v , let $I_v \subset \{1, \dots, r\}$ be the set of indices such that $b_i(x)$ does not intersect the connected component of the original component (see Definition 4.3) in $X \setminus \{v\}$. Let C_v be a choice of a simple loop in $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ such that in one connected component of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus C_v$ contains $\{b_i(c) | i \in I_v\}$, and the other contains $\{b_i(c) | i \notin I_v\}$. I further require that the C_v 's are chosen so that C_v does not intersect C_w for $v \neq w$.

For our given i , there is a series of $\mathbb{P}_{\mathbb{C}}^1$'s in \hat{X} that connects the $\mathbb{P}_{\mathbb{C}}^1$ that meets $b_i(x)$ with the original component (see Definition 4.3). Call these components X_1, \dots, X_{N_i} (each one is just a $\mathbb{P}_{\mathbb{C}}^1$, and X_{N_i} is the original component). Define θ_l (for $l = 1, \dots, N_{i-1}$) to be the thickness of the node that connects X_l with X_{l+1} . (See Definition 4.4.) Define I_l to be $\{j \in \{1, \dots, r\} | b_j(x) \text{ meets } X_1 \cup \dots \cup X_l\}$.

Lastly, define for every subset $J \subset \{1, \dots, r\}$ an element $q_J := \prod_{j \in J} \alpha_j$ (where the order of the product is the order of the integers in J).

Theorem 5.1. *In the situation above, the element \mathcal{D} acts on α_i by mapping it to ${}^q\alpha_i = q\alpha_i q^{-1}$, where $q = q_{I_{N_{i-1}}}^{\theta_{N_{i-1}}} \cdots q_{I_1}^{\theta_1}$.*

Proof. It follows from Theorem 4.5 that \mathcal{D} acts on $\alpha_1, \dots, \alpha_r$ by $\prod_v D_v^{\theta_v}$, where D_v is the Dehn twist around C_v . We may deform $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}}$ continuously so that $b_1(c), \dots, b_r(c)$ move to $1, \dots, r$, and the base point moves to 0. Furthermore, this deformation can be chosen so that each circle C_v deforms to a circle C'_v which does not intersect the line $\{j + a\sqrt{-1} | a \in \mathbb{R}\}$ for any $j \notin I_v$. Let D'_v be the Dehn twist along C'_v . Let $\alpha'_1, \dots, \alpha'_r$ be the loops of $\pi_1((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{1, \dots, r\}, 0)$ that arise by deforming $\alpha_1, \dots, \alpha_r$. By deforming again, one can assume without loss of generality that α'_j is the loop given by concatenating the following paths:

- (1) $\sqrt{-1}t$ for $0 \leq t \leq 1$.
- (2) $\sqrt{-1} + jt$ for $0 \leq t \leq 1$.
- (3) $(1 - \frac{t}{2})\sqrt{-1} + j$ for $0 \leq t \leq 1$.
- (4) $\frac{1}{2}e^{(\frac{\pi}{2} + 2\pi t)\sqrt{-1}} + j$ for $0 \leq t \leq 1$.

- (5) $(1 - \frac{1-t}{2})\sqrt{-1} + j$ for $0 \leq t \leq 1$.
- (6) $\sqrt{-1} + j(1-t)$ for $0 \leq t \leq 1$.
- (7) $\sqrt{-1}(1-t)$ for $0 \leq t \leq 1$.

Clearly, it suffices to describe the action of $\prod_v (D'_v)^{\theta_v}$ on $\alpha'_1, \dots, \alpha'_r$.

Note that the α'_i 's can be expressed in terms of the q_i 's in Figure 2 of [6] as $q_1 \cdots q_{i-1} (q_i^{-1})$. Proposition 2.8 in [6] describes the action of $D'_v{}^{-1}$ on q_1, \dots, q_r . In the terminology of [6], $D'_v{}^{-1} = D_{[I_v, \emptyset, \emptyset]}$. Therefore, D'_v takes q_i to q_i if i is not in I_v , and it takes it to $q_i^{\prod_{j \in I_v} q_j}$ if i is in I_v . An easy computation shows that this implies that D'_v takes α'_i to α'_i if i is not in I_v , and it takes α'_i to $\prod_{j \in I_v} \alpha'_j \alpha'_i$ if i is in I_v .

It remains to describe the action of $\prod_v (D'_v)^{\theta_v}$ on $\alpha'_1, \dots, \alpha'_r$. Since we know the action of each D'_v , this reduces to an easy verification. \square

Remark 5.2. In Flon's paper ([6]), the convention on the direction of the Dehn twists is reverse from the convention here.

Corollary 5.3. *Let K be a strictly henselian field of characteristic 0, residue characteristic p , and parameter t . Let G be a finite prime-to- p group. Then for every G -Galois branched cover of \mathbb{P}_K^1 , ramified only over K -rational points, its field of moduli relative to K is contained in $K(t^{\frac{1}{N}})$, where $N = \exp(\text{Inn}(G))$. (In particular, this implies that t is tamely ramified in the field of moduli relative to K .)*

Proof. Let a_1, \dots, a_r be K -rational points of \mathbb{P}_K^1 . Let \bar{o} be a \bar{K} -point of $\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}$ lying over a K -rational point. Let a G -Galois branched cover of \mathbb{P}_K^1 be given by a surjection $\rho : \pi'(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \twoheadrightarrow G$. Let $\alpha_1, \dots, \alpha_r$ be as in Theorem 5.1, applied to $K(t^{\frac{1}{N}})$. Then it suffices to prove to prove that $(\rho(\delta \alpha_1), \dots, \rho(\delta \alpha_r))$ is uniformly conjugate to $(\rho(\alpha_1), \dots, \rho(\alpha_r))$. In the terminology of Theorem 5.1, each θ_i is divisible by N . Since $\text{Inn}(G)$ is isomorphic to $G/Z(G)$, this implies that $\rho(q_{I_{N_i-1}}^{\theta_{N_i-1}} \cdots q_{I_1}^{\theta_1})$ is in the center of G . In particular we have that $\rho(q_{I_{N_i-1}}^{\theta_{N_i-1}} \cdots q_{I_1}^{\theta_1} \alpha_i) = \rho(\alpha_i)$ for $i = 1, \dots, r$. Since, by Theorem 5.1, δ acts on α_i by taking it to $q_{I_{N_i-1}}^{\theta_{N_i-1}} \cdots q_{I_1}^{\theta_1} \alpha_i$, the field of moduli is contained in $K(t^{\frac{1}{N}})$. \square

Remark 5.4. With some work one can show that Théorèmes 3.2 and 3.7 in [13], adapted to our situation, imply that in the situation above the field of moduli is contained in $K(t^{\frac{1}{M}})$, where $M = \exp(G)$. The corollary above is a strengthening of this result.

6. THE PROOF OF THEOREM 3.1

Corollary 5.3 above will help us prove Lemma 6.1 below, which in turn will allow us to prove the symmetric version of Proposition 4.1, namely Theorem 3.1.

Lemma 6.1. *In the situation of Theorem 3.1, the following hold:*

- (1) *The sequence of morphisms*

$$\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\} \rightarrow \mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\} \rightarrow \text{Spec}(K)$$

induces a short exact sequence

$$1 \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \text{Gal}(K)^{(p')} \rightarrow 1.$$

(2) *The sequence of morphisms*

$$(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\} \rightarrow \mathcal{T} \rightarrow B \setminus \{0\}$$

induces a short exact sequence

$$1 \rightarrow \hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)^{(p')} \rightarrow \hat{\pi}_1^{\text{top}}(\mathcal{T}, (u, c))^{(p')} \rightarrow \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')} \rightarrow 1.$$

Proof. Since taking maximal prime-to- p quotients is a right exact functor, we have the induced short exact sequences

$$\hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, u)^{(p')} \rightarrow \hat{\pi}_1^{\text{top}}(\mathcal{T}, (u, c))^{(p')} \rightarrow \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')} \rightarrow 1$$

$$\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \text{Gal}(K)^{(p')} \rightarrow 1.$$

Note that Corollary 5.5.8 in [15], which gives a condition for the injectivity of maps of fundamental groups, works for every Galois category (it is only stated there for the Galois category of finite étale covers). Therefore in order to prove the first claim it suffices to prove that for every prime-to- p group G , and for every G -Galois étale cover of $\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}$, there is a field of definition that has a prime-to- p degree over K . This fact is contained in the statement of Lemma 5.3.

Similarly, to prove the second claim it suffices to prove that every prime-to- p normal covering space of $(\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}$ with deck transformation group G extends to one over $((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \times (B' \setminus \{0\})) \setminus \{(b_i(y), y) | y \in B' \setminus \{0\}\}_i$, where B' is a covering space of B given by $y^n = x$ such that n is a natural number coprime to p . This follows from the proof of Lemma 5.3. \square

We are now ready to prove 3.1.

Proof. (Theorem 3.1) The first claim of Theorem 3.1 is precisely the first claim of Proposition 4.1, and has therefore already been proven.

In order to prove Claims 2 and 3, observe the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \rightarrow & \hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u) & \xrightarrow{f_1} & \hat{\pi}_1^{\text{top}}(\mathcal{T}, (u, c)) & \xrightarrow{g_1} & \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c) \rightarrow 1 \\ & & \downarrow \gamma_1 & & \downarrow \gamma_2 & & \downarrow \gamma_3 \\ 1 & \rightarrow & \hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')} & \xrightarrow{f_2} & \hat{\pi}_1^{\text{top}}(\mathcal{T}, (u, c))^{(p')} & \xrightarrow{g_2} & \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)^{(p')} \rightarrow 1 \end{array}$$

Let s_1 be the section of g_1 induced by the point (u, c) . The action of $\sigma \in \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)$ on $\gamma_1(a) \in \hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)^{(p')}$ is given by $\gamma_1(f_1^{-1}(s_1(\sigma)f_1(a)s_1(\sigma)^{-1}))$. It is well defined because the monodromy action doesn't change the degree of the cover. Let s_2 be the section of g_2 induced by the point (u, c) by virtue of the functoriality of taking maximal prime-to- p quotients. It is easy to see that $s_2 \circ \gamma_3 = \gamma_2 \circ s_1$. Furthermore, since f_2 is injective (Lemma 6.1) then $\gamma_1 \circ f_1^{-1} = f_2^{-1} \circ \gamma_2$ on $\text{Im}(f_1)$. Therefore:

$$\begin{aligned} \gamma_1(f_1^{-1}(s_1(\sigma)f_1(a)s_1(\sigma)^{-1})) &= f_2^{-1}(\gamma_2(s_1(\sigma)f_1(a)s_1(\sigma)^{-1})) = \\ &= f_2^{-1}(s_2(\gamma_3(\sigma))\gamma_2(f_1(a))s_2(\gamma_3(\sigma))^{-1}) \end{aligned}$$

This implies that the action of $\sigma \in \hat{\pi}_1^{\text{top}}(B \setminus \{0\}, c)$ on a depends only on $\gamma_3(\sigma)$, which proves the second claim of Theorem 3.1 (i.e., define $\rho_1(\gamma_3(\sigma))$ to be the automorphism taking $\gamma_1(a)$ to $\gamma_1(f_1^{-1}(s_1(\sigma)f_1(a)s_1(\sigma)^{-1}))$, for every $a \in \hat{\pi}_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{b_1(c), \dots, b_r(c)\}, u)$). Let $\phi_1 : \hat{\pi}_1(B \setminus \{0\}, c)^{(p')} \rightarrow \text{Gal}(K)^{(p')}$ be the map that takes the image of \mathcal{D} in $\hat{\pi}_1(B \setminus \{0\}, c)^{(p')}$ to the element in $\text{Gal}(K)^{(p')}$ that takes $t_m^{\frac{1}{m}}$ to $e^{\frac{2\pi\sqrt{-1}}{m}}t_m^{\frac{1}{m}}$ for every m coprime to p . Since ρ_1 and ϕ_1 factor as the

quotient map $\hat{\pi}_1(B \setminus \{0\}, c) \rightarrow \hat{\pi}_1(B \setminus \{0\}, c)^{(p')}$ composed with ρ'_1 or ϕ'_1 resp., Proposition 4.1 proves the commutativity of the diagram in the third claim of Theorem 3.1. \square

7. EXAMPLES

In the situation of Theorem 3.1, Section 5 gives us an explicit description of the action of $\text{Gal}(K)$ on $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$. By Lemma 6.1, we have a short exact sequence:

$$1 \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \rightarrow \text{Gal}(K)^{(p')} \rightarrow 1.$$

Let $s' : \text{Gal}(K)^{(p')} \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ be the section induced by \bar{o} , and let $\delta \in \text{Gal}(K)^{(p')}$ be the element that takes $t^{\frac{1}{m}}$ to $e^{\frac{2\pi\sqrt{-1}}{m}} t^{\frac{1}{m}}$ for every natural number m coprime to p . Let $\alpha_1, \dots, \alpha_r$ be a bouquet of loops around a_1, \dots, a_r . We have that $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \cong \langle \alpha_1, \dots, \alpha_r | \widehat{\alpha_1 \cdots \alpha_r} = 1 \rangle^{(p')}$. Let β_i be $s'(\delta)\alpha_i$. It is clear from the description of this action in Section 5 that the β_i 's are in the image of the map $\langle \alpha_1, \dots, \alpha_r | \alpha_1 \cdots \alpha_r = 1 \rangle \rightarrow \langle \alpha_1, \dots, \alpha_r | \widehat{\alpha_1 \cdots \alpha_r} = 1 \rangle^{(p')}$. The following lemma allows us to describe $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ as the maximal prime-to- p quotient of a profinite completion of a semi-direct product.

Lemma 7.1. *Let A and B be finitely generated free groups, and let p be a prime. Let $\omega_1 : B \rightarrow \text{Aut}(A)$ be a homomorphism that extends (A and B are in particular residually finite, and therefore embed into their profinite completions) to a continuous homomorphism $\omega_2 : \hat{B} \rightarrow \text{Aut}(\hat{A})$. Furthermore, assume that $\hat{A} \rtimes_{\omega_2} \hat{B}$ is a pro-finite group. Then*

$$\widehat{A \rtimes_{\omega_1} B} \cong \hat{A} \rtimes_{\omega_2} \hat{B}.$$

Furthermore, if we assume that the natural homomorphism $\hat{A}^{(p')} \rightarrow (\hat{A} \rtimes_{\omega_2} \hat{B})^{(p')}$ is injective, then ω_2 induces a well-defined homomorphism $\omega_3 : \hat{B}^{(p')} \rightarrow \text{Aut}(\hat{A}^{(p')})$, and

$$\widehat{A \rtimes_{\omega_1} B}^{(p')} \cong \hat{A}^{(p')} \rtimes_{\omega_3} \hat{B}^{(p')}.$$

Proof. Let n be a natural number, and let A_n be the intersection of all index n subgroups of A . It is easy to see that A_n is characteristic in A . Let N be some normal subgroup of B of finite index. It is easy to check that

$$1 \rightarrow A/A_n \rightarrow (A \rtimes_{\omega_1} B)/A_n N \rightarrow B/N \rightarrow 1$$

is a well-defined short exact sequence.

By taking inverse limits, we get the following short exact sequence:

$$1 \rightarrow \hat{A} \rightarrow \varprojlim (A \rtimes_{\omega_1} B)/A_n N \rightarrow \hat{B} \rightarrow 1.$$

The exactness on the right is due to the compatibility of the sections of

$$1 \rightarrow A/A_n \rightarrow (A \rtimes_{\omega_1} B)/A_n N \rightarrow B/N \rightarrow 1$$

as N and A_n vary.

Since for every finite index subgroup of $A \rtimes_{\omega_1} B$ there exists a natural number n and a normal subgroup N of B such that it contains $A_n N$, it follows that

$$\varprojlim (A \rtimes_{\omega_1} B)/A_n N \cong \widehat{A \rtimes_{\omega_1} B}.$$

It remains to show that $\varprojlim (A \rtimes_{\omega_1} B)/A_n N \cong \hat{A} \rtimes_{\omega_2} \hat{B}$.

Similarly to the computation above, since \hat{A}_n is invariant under continuous automorphisms of \hat{A} , and since \hat{N} is a normal open subgroup of \hat{B} , the homomorphisms

$$1 \rightarrow \hat{A}/\hat{A}_n \rightarrow (\hat{A} \rtimes_{\omega_2} \hat{B})/\hat{A}_n \hat{N} \rightarrow \hat{B}/\hat{N} \rightarrow 1$$

form a well-defined short exact sequence.

This short exact sequence fits into the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & A/A_n & \longrightarrow & (A \rtimes_{\omega_1} B)/A_n N & \longrightarrow & B/N \longrightarrow 1 \\ & & \downarrow \gamma_1 & & \downarrow \gamma_2 & & \downarrow \gamma_3 \\ 1 & \longrightarrow & \hat{A}/\hat{A}_n & \longrightarrow & (\hat{A} \rtimes_{\omega_2} \hat{B})/\hat{A}_n \hat{N} & \longrightarrow & \hat{B}/\hat{N} \longrightarrow 1 \end{array}$$

Since γ_1 and γ_3 are isomorphisms, the Five Lemma implies that γ_2 is also an isomorphism. Therefore, we have a short exact sequence

$$1 \rightarrow \hat{A} \rightarrow \varprojlim (\hat{A} \rtimes_{\omega_2} \hat{B})/\hat{A}_n \hat{N} \rightarrow \hat{B} \rightarrow 1.$$

Since the $\hat{A}_n \hat{N}$'s are open normal subgroups of $\hat{A} \rtimes_{\omega_2} \hat{B}$, and since $\hat{A} \rtimes_{\omega_2} \hat{B}$ is pro-finite, the universal property of inverse limits gives us the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \hat{A} & \longrightarrow & \varprojlim (\hat{A} \rtimes_{\omega_2} \hat{B})/\hat{A}_n \hat{N} & \longrightarrow & \hat{B} \longrightarrow 1 \\ & & \downarrow & & \downarrow \gamma & & \downarrow \\ 1 & \longrightarrow & \hat{A} & \longrightarrow & \hat{A} \rtimes_{\omega_2} \hat{B} & \longrightarrow & \hat{B} \longrightarrow 1 \end{array}$$

Since the vertical homomorphisms on the rightmost and the leftmost are isomorphisms, it follows from the Five Lemma that γ is also an isomorphism. Therefore:

$$\widehat{A \rtimes_{\omega_1} B} \cong \varprojlim (A \rtimes_{\omega_1} B)/A_n N \cong \varprojlim (\hat{A} \rtimes_{\omega_2} \hat{B})/\hat{A}_n \hat{N} \cong \hat{A} \rtimes_{\omega_2} \hat{B}$$

as we wanted to show. It follows immediately from the functoriality of taking prime-to- p quotients that if the induced exact sequence

$$\hat{A}^{(p')} \rightarrow (\hat{A} \rtimes_{\omega_2} \hat{B})^{(p')} \rightarrow \hat{B}^{(p')} \rightarrow 1$$

is injective on the left, then $\hat{A}^{(p')} \rtimes_{\omega_3} \hat{B}^{(p')} \cong (\hat{A} \rtimes_{\omega_2} \hat{B})^{(p')}$ where ω_3 is induced by ω_2 . Since by the first claim $\hat{A} \rtimes_{\omega_2} \hat{B} \cong \widehat{A \rtimes_{\omega_1} B}$ the lemma follows. \square

It follows from Lemma 7.1 and the discussion above it that

$$\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \cong \langle \alpha_1, \dots, \widehat{\alpha_r}, \delta | \delta \alpha_i = \beta_i \rangle^{(p')}.$$

Using this, and Section 5, we can easily compute prime-to- p fundamental groups.

Example 7.2. *The prime-to- p étale fundamental group $\pi'_1(\mathbb{P}_{\mathbb{Q}_p^{\text{un}}}^1 \setminus \{a_1, \dots, a_r\})$, where a_1, \dots, a_r are \mathbb{Q}_p^{un} -rational points of $\mathbb{P}_{\mathbb{Q}_p^{\text{un}}}^1$ that don't coalesce on the special fiber of $\mathbb{P}_{\mathbb{Z}_p^{\text{un}}}^1$, is isomorphic to $\langle \alpha_1, \dots, \alpha_r, \delta | \widehat{\alpha_1 \cdots \alpha_r} = 1, \forall i \delta \alpha_i = \alpha_i \delta \rangle^{(p')}$.*

Example 7.3. *For a prime $p \geq 3$, and a natural number m , we have that*

$$\pi'_1(\mathbb{P}_{\mathbb{Q}_p^{\text{un}}}^1 \setminus \{0, p^m, 1, 2\}) \cong$$

$$\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \delta | \alpha_1 \cdots \alpha_4 = 1, \delta \alpha_1 = \widehat{(\alpha_1 \alpha_2)^m} \alpha_1, \delta \alpha_2 = (\alpha_1 \alpha_2)^m \alpha_2, \delta \alpha_3 = \alpha_3, \delta \alpha_4 = \alpha_4 \rangle^{(p')}$$

8. LOCAL-GLOBAL PRINCIPLE FOR FIELDS OF MODULI

Although variants of the theorem of this section have been known to experts, its proof has not appeared in the literature to the best of the author's knowledge.

Let p be a prime, and let \mathbb{Q}_p be the field of p -adic numbers. Let $\mathbb{Q}_p^{\text{alg}}$ denote the field of algebraic p -adics, i.e. the subfield of \mathbb{Q}_p of algebraic elements over \mathbb{Q} . Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}_p^{\text{alg}}$. Let $\mathbb{Z}_p^{\text{alg}}$ be the integral closure of \mathbb{Z} in $\mathbb{Q}_p^{\text{alg}}$, and $\bar{\mathbb{Z}}$ be the integral closure of \mathbb{Z} in $\bar{\mathbb{Q}}$. Let $\bar{\mathbb{Z}}_p$ be defined as $\varprojlim \mathbb{Z}_p^{\text{alg}} / (p\mathbb{Z}_p \cap \mathbb{Z}_p^{\text{alg}})^n$. Let $\bar{\mathbb{Q}}_p$ be the quotient field of $\bar{\mathbb{Z}}_p$. It is clear that \mathbb{Z}_p embeds naturally into $\bar{\mathbb{Z}}_p$. This embedding induces an embedding of \mathbb{Q}_p into $\bar{\mathbb{Q}}_p$. It is easy to see that via this embedding $\bar{\mathbb{Q}}_p$ is an algebraic closure of \mathbb{Q}_p .

Let \mathcal{P} be the set of primes of $\text{Spec}(\bar{\mathbb{Z}})$ lying above the prime $p\mathbb{Z}_p \cap \mathbb{Z}_p^{\text{alg}}$ of $\text{Spec}(\mathbb{Z}_p^{\text{alg}})$.

In order to prove the first theorem of this section we require a lemma. In the lemma below $\text{Hom}_A(B, C)$ means the set of morphisms from B to C in the category of A -algebras.

Lemma 8.1. *Let $F \subset E, L$ be fields. Then there is a bijection $\text{Hom}_L(L \otimes_F E, L) \rightarrow \text{Hom}_F(E, L)$ given by $\alpha \mapsto (e \mapsto \alpha(1 \otimes e))$.*

Proof. It is clear that the map $\text{Hom}_F(E, L) \rightarrow \text{Hom}_L(L \otimes_F E, L)$ given by taking ϕ to the unique homomorphism that takes $l \otimes e$ to $l \otimes \phi(e)$ is an inverse. \square

Let \mathfrak{p} be a prime in \mathcal{P} . Note that there is a natural homomorphism $\beta_{\mathfrak{p}} : \bar{\mathbb{Z}}_p = \varprojlim \mathbb{Z}_p^{\text{alg}} / (p\mathbb{Z}_p \cap \mathbb{Z}_p^{\text{alg}})^n \rightarrow \varprojlim \bar{\mathbb{Z}} / \mathfrak{p}^n$ given by embedding coordinate-wise. It is easy to see that this homomorphism is in fact an isomorphism. Therefore $\beta_{\mathfrak{p}}$ extends to an isomorphism of $\bar{\mathbb{Q}}_p$ with $\text{Quot}(\varprojlim \bar{\mathbb{Z}} / \mathfrak{p}^n)$ (which fixes $\mathbb{Q}_p^{\text{alg}}$ pointwise as a subfield of both). I will continue to denote this extension $\beta_{\mathfrak{p}}$. Let $\alpha : \mathcal{P} \rightarrow \text{Hom}_{\mathbb{Q}_p^{\text{alg}}}(\bar{\mathbb{Q}}, \bar{\mathbb{Q}}_p)$ be the mapping that takes $\mathfrak{p} \in \mathcal{P}$ to the composition of $\bar{\mathbb{Q}} \rightarrow \text{Quot}(\varprojlim \bar{\mathbb{Z}} / \mathfrak{p}^n)$ (induced by the homomorphism $\bar{\mathbb{Z}} \rightarrow \varprojlim \bar{\mathbb{Z}} / \mathfrak{p}^n$ given by the diagonal), and $\beta_{\mathfrak{p}}^{-1}$.

Theorem 8.2. *In the situation above, the mapping α is a bijection between \mathcal{P} and $\text{Hom}_{\mathbb{Q}_p^{\text{alg}}}(\bar{\mathbb{Q}}, \bar{\mathbb{Q}}_p)$.*

Proof. By Lemma 8.1 with $L = \mathbb{Q}_p$, $\bar{L} = \bar{\mathbb{Q}}_p$, $F = \mathbb{Q}_p^{\text{alg}}$, and $E = \bar{\mathbb{Q}}$, we see that $\text{Hom}_{\mathbb{Q}_p^{\text{alg}}}(\bar{\mathbb{Q}}, \bar{\mathbb{Q}}_p)$ is bijective with $\text{Hom}_{\bar{\mathbb{Q}}_p}(\bar{\mathbb{Q}}_p \otimes_{\mathbb{Q}_p^{\text{alg}}} \bar{\mathbb{Q}}, \bar{\mathbb{Q}}_p)$. We proceed to describe the latter set.

Let $\text{Spec}(\bar{\mathbb{Z}} \otimes_{\mathbb{Z}_p^{\text{alg}}} \bar{\mathbb{Z}}_p) \rightarrow \text{Spec}(\bar{\mathbb{Z}}_p)$ be the base change of $\text{Spec}(\bar{\mathbb{Z}}) \rightarrow \text{Spec}(\mathbb{Z}_p^{\text{alg}})$ to a formal local neighborhood of $p\mathbb{Z}_p \cap \mathbb{Z}_p^{\text{alg}}$. It is clear that $\bar{\mathbb{Z}} \otimes_{\mathbb{Z}_p^{\text{alg}}} \bar{\mathbb{Z}}_p$ is isomorphic to $\bigoplus_{\mathfrak{p} \in \mathcal{P}} \bar{\mathbb{Z}}_p$. By base changing to the generic point of $\bar{\mathbb{Z}}_p$, we get the morphism $\text{Spec}(\bar{\mathbb{Z}} \otimes_{\mathbb{Z}_p^{\text{alg}}} \bar{\mathbb{Q}}_p) \rightarrow \text{Spec}(\bar{\mathbb{Q}}_p)$. Note that

$$\bar{\mathbb{Z}} \otimes_{\mathbb{Z}_p^{\text{alg}}} \bar{\mathbb{Q}}_p \cong \bigoplus_{\mathfrak{p} \in \mathcal{P}} (\bar{\mathbb{Z}}_p \otimes_{\bar{\mathbb{Z}}_p} \bar{\mathbb{Q}}_p) \cong \bigoplus_{\mathfrak{p} \in \mathcal{P}} \bar{\mathbb{Q}}_p.$$

Since $\text{Hom}_{\bar{\mathbb{Q}}_p}(\bigoplus_{\mathfrak{p} \in \mathcal{P}} \bar{\mathbb{Q}}_p, \bar{\mathbb{Q}}_p)$ is bijective to \mathcal{P} , this proves the theorem. \square

Theorem 8.3. *In the situation above, let $X_{\bar{\mathbb{Q}}} \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}}^1$ be a G -Galois branched cover with field of moduli K relative to \mathbb{Q} . Let \mathfrak{p} be a prime in \mathcal{P} , and let $\alpha(\mathfrak{p}) : \bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_p$ be its corresponding embedding via Theorem 8.2. Let \mathfrak{q} be $\mathfrak{p} \cap K$. Let K' be the field of moduli of the base change $X_{\bar{\mathbb{Q}}} \times_{\bar{\mathbb{Q}}} \bar{\mathbb{Q}}_p \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}_p}^1$ relative to \mathbb{Q}_p . Then the index of ramification of p in K' is equal to the index of ramification of \mathfrak{q} over p .*

Proof. Let e' be the index of ramification of K'/\mathbb{Q}_p , and let e be the index of ramification of \mathfrak{q} over p in the field extension K/\mathbb{Q} .

By assumption K' is a subfield of $\mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e'}})$, where $p^{\frac{1}{e'}}$ is some e'^{th} root of p in $\bar{\mathbb{Q}}_p$. Since $\mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e'}})$ has cohomological dimension 1, it follows that it is in fact a field of definition of $X_{\bar{\mathbb{Q}}} \times_{\bar{\mathbb{Q}}} \bar{\mathbb{Q}}_p \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}_p}^1$.

By Artin's Algebraization Theorem ([1]), it follows that $\mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e'}}) \cap \bar{\mathbb{Q}}$ is also a field of definition. Since the cover is defined by finitely many polynomials, it is in fact defined over some number field $L \subset \mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e'}}) \cap \bar{\mathbb{Q}}$. Since K is the intersection of all fields of definition of $X_{\bar{\mathbb{Q}}} \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}}^1$ (see [4]), it follows that K is a subfield of L . Therefore, we have that $\mathfrak{q} \subset p^{\frac{1}{e'}} \mathbb{Z}_p^{\text{un}}(p^{\frac{1}{e'}}) \cap K$. It follows that $e \leq e'$.

Let $p^{\frac{1}{e}}$ be some e^{th} root of p in $\bar{\mathbb{Q}}_p$. Notice that $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e}}))$ is isomorphic to the inertia subgroup of \mathfrak{a} in $\text{Gal}(\bar{\mathbb{Q}}/K)$. Therefore the field of moduli of $X_{\bar{\mathbb{Q}}} \times_{\bar{\mathbb{Q}}} \bar{\mathbb{Q}}_p \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}_p}^1$ relative to \mathbb{Q}_p is contained in $\mathbb{Q}_p^{\text{un}}(p^{\frac{1}{e}})$. Therefore $e' \leq e$, proving the theorem. \square

9. GLOBAL RESULTS ON RAMIFICATION IN THE FIELD OF MODULI

Theorem 3.1 together with Theorem 8.3 suggest that by choosing \mathbb{Q} -rational points a_1, \dots, a_r of $\mathbb{P}_{\mathbb{Q}}^1$ carefully, we would be able to construct Galois covers of $\mathbb{P}_{\mathbb{Q}}^1$ with desirable fields of moduli. Theorems 9.1 and 9.6 in this section give global points with desirable local behavior.

Theorem 9.1. *Let G be a finite group. Then for every positive integer r there is a set $T = \{a_1, \dots, a_r\}$ of closed points of $\mathbb{P}_{\mathbb{Q}}^1$, such that every G -Galois branched cover of $\mathbb{P}_{\mathbb{Q}}^1$ that is ramified only over T , has a field of moduli that is unramified (over \mathbb{Q}) outside of the primes dividing $|G|$.*

Proof. Let p be a prime that divides $|G|$, and let n be a natural number such that $r \leq p^n$. Take T to be any subset with cardinality r of the set of $(p^n)^{\text{th}}$ roots of unity 1. It is easy to check that these points, viewed as horizontal divisors in $\mathbb{P}_{\mathbb{Z}}^1$, coalesce only over the prime p . Therefore, by Beckmann's result, we're done. \square

Note that in Theorem 9.1 we put no restrictions on the branch points. Theorem 9.6 gives a global result if we further ask that the branch points be rational. In order to discuss the proof of Theorem 9.6, we need a few definitions.

Definition 9.2. *Local data $(V, v_0, E, \epsilon, \eta)$ at p with r marks is a tree (V, E) equipped with the following extra structure:*

- A distinguished vertex $v_0 \in V$ (which we call the “root”)
- A function $\epsilon : \{1, \dots, r\} \rightarrow V$
- A function $\eta : E \rightarrow \mathbb{N}$

such that for every vertex v , we have that $3 \leq \deg(v) + |\epsilon^{-1}(\{v\})| \leq p + 1$.

Furthermore, for every $e \in E$ we will say that $\eta(e)$ is the thickness of e .

Definition 9.3. *For \mathbb{Q} -rational points a_1, \dots, a_r of $\mathbb{P}_{\mathbb{Q}}^1$, and for p a prime of \mathbb{Z} , we define the induced local data with r marks at p as the $(V, v_0, E, \epsilon, \eta)$ defined as follows:*

- The set of vertices V is the set of components of the closed fiber of the stable marked model of $\mathbb{P}_{\mathbb{Z}_p}^1$ with marks $\{a_1, \dots, a_r\}$.
- The root v_0 is the original component (see Definition 4.3).
- The set of edges E connects two vertices if and only if there is a node connecting them in the stable reduction.
- The function ϵ assigns to i the irreducible component that meets a_i .
- The function η assigns to e the thickness of its corresponding node.

In order to speak comfortably about local data, we will require some terminology.

Definition 9.4. *Let $(V, v_0, E, \epsilon, \eta)$ be local data at some prime p with r marks. For every vertex v define its minimal path T_v to be the set of edges from the root to the vertex. The tail of an edge*

e will mean the vertex lying on e that is closest to the root, and the head of e will mean the vertex on e that is farthest from the root.

The following lemma will play a big role in the proof of Theorem 9.6.

Lemma 9.5. (*local-global result*) *Let $S \subset \text{Spec}(\mathbb{Z})$ be a finite set of primes, and let r be a natural number. For every prime p in S let $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ be local data with r marks. Then there exist \mathbb{Q} -rational points a_1, \dots, a_r of $\mathbb{P}_{\mathbb{Q}}^1$ that induce the local data with r marks $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ for every prime p of S .*

Proof. We will do this by induction on $|S|$. Assume first that $|S| = 1$, and denote by p the only element of S .

For the sake of simplicity, I will deal first with the case that the root has less than $p + 1$ edges coming out of it. Let $c : E_p \rightarrow \{0, \dots, p-1\}$ be some function that satisfies that if e and e' are edges that share a tail then $c(e) \neq c(e')$. Let $k : \{1, \dots, r\} \rightarrow \{0, \dots, p-1\}$ be some function that satisfies that if $\epsilon_p(i) = \epsilon_p(j)$ then $k(i) \neq k(j)$; and that for every $i \in \{1, \dots, r\}$, and every edge e whose tail is $\epsilon_p(i)$, we have $k(i) \neq c(e)$. For every vertex v let $T_v = (e_1, \dots, e_d)$ be the set of edges in the minimal path between the root and v , ordered from the edge closest to the root, to the edge farthest from the root.

Let

$$a_i = c(e_1) + c(e_2)p^{\eta_p(e_1)} + c(e_3)p^{\eta_p(e_1)+\eta_p(e_2)} + \dots + c(e_d)p^{\eta_p(e_1)+\dots+\eta_p(e_{d-1})} + k(\epsilon_p(i))p^{\eta_p(e_1)+\dots+\eta_p(e_d)}$$

where e_1, \dots, e_d are the edges leading from the root to the vertex $\epsilon_p(i)$ in that order. It is easy to see that this choice induces the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$.

We now describe the situation where the root has $p + 1$ edges coming out of it. Let e be some edge whose head is the root. Removing e from the local data gives two trees. The tree that contains the root induces local data $(V'_p, v'_{0,p}, E'_p, \epsilon'_p, \eta'_p)$. The tree which does not contain the root induces local data $(V''_p, v''_{0,p}, E''_p, \epsilon''_p, \eta''_p)$ by setting the tail of e as the root. As $(V'_p, v'_{0,p}, E'_p, \epsilon'_p, \eta'_p)$ satisfies that it has p edges coming out of its root, we may execute the algorithm described above to get global points $a_1, \dots, a_l \in \mathbb{Q}$. The local data $(V''_p, v''_{0,p}, E''_p, \epsilon''_p, \eta''_p)$ also satisfies that it has $\leq p$ edges coming out of its root, and so we may again execute the algorithm above to get global points $a'_{l+1}, \dots, a'_r \in \mathbb{Q}$. Let a_{l+1}, \dots, a_r be $1/p^{\eta_p(e)}a'_{l+1}, \dots, 1/p^{\eta_p(e)}a'_r$ respectively. It is easy to check that a_1, \dots, a_r induce the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ at p .

We now proceed by induction. Assume that b_1, \dots, b_r are global points that induce the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ for every $p \in S \setminus \{q\}$. We will prove that there are global points a_1, \dots, a_r that induce the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ for every $p \in S$.

A key fact is that there exists a natural number M_p such that if a_1, \dots, a_r are global points such that $a_1 \equiv b_1 \pmod{p^{M_p}}$ then a_1, \dots, a_r induces the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ as well. Indeed, this M_p be chosen to be $1 + \max_{i \neq j} v_{0,p}(b_i - b_j)$.

Let c_1, \dots, c_r be global points that induce the local data $(V_q, v_{0,q}, E_q, \epsilon_q, \eta_q)$ at q . In light of the above, it suffices to find a_1, \dots, a_r such that $a_i \equiv b_i \pmod{\prod_{p \in S \setminus \{q\}} p^{M_p}}$, and $a_i \equiv c_i \pmod{q^{M_q}}$. The existence of a_1, \dots, a_r with these properties follows from the Chinese Remainder Theorem. \square

Finally, we are ready for Theorem 9.6.

Theorem 9.6. *Let G be a finite group. Then for every positive integer r , and for every finite set S of rational primes that don't divide $|G|$, there is a choice of \mathbb{Q} -rational points $T = \{a_1, \dots, a_r\}$*

such that every G -Galois étale cover of $\mathbb{P}_{\mathbb{Q}}^1 \setminus T$ has a field of moduli M that is unramified over the primes of S .

Proof. For every p in S , let $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ be local data at p such that all of the thicknesses are divisible by $\exp(\text{Inn}(G))$. By Lemma 9.5, there exist global points a_1, \dots, a_r that induce the local data $(V_p, v_{0,p}, E_p, \epsilon_p, \eta_p)$ at p , for every p in S . The theorem now follows from Theorem 8.3 and Corollary 5.3. \square

10. VERTICAL RAMIFICATION

In this section we draw inspiration from Theorem 3.1, and prove a generalization of the following Theorem by Beckmann ([2]) on vertical ramification:

Theorem 10.1. (*Beckmann*) *Let K be the quotient field of a strictly henselian DVR R , of characteristic 0, residue characteristic $p \geq 0$ and uniformizing parameter t . Let a_1, \dots, a_r be K -rational non-coalescing points on \mathbb{P}_K^1 . Then for every centerless group G of order prime to p , and every regular G -Galois branched cover of \mathbb{P}_K^1 ramified only over a_1, \dots, a_r , the induced cover of \mathbb{P}_R^1 has no vertical ramification (i.e., the divisor t of \mathbb{P}_R^1 is unramified).*

Let K be the quotient field of a strictly henselian DVR R , of characteristic 0, residue characteristic $p \geq 0$ and uniformizing parameter t . Fix an embedding of \bar{K} into \mathbb{C} . Let a_1, \dots, a_r be K -rational points on \mathbb{P}_K^1 . Let $\delta \in \text{Gal}(K)^{(p')}$ be the element such that $t^{\frac{1}{m}} \mapsto e^{\frac{2\pi\sqrt{-1}}{m}} t^{\frac{1}{m}}$ for every m coprime to p . Let \bar{o} be a \mathbb{C} -point of $\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}$ lying over a K -rational point whose Zariski closure in \mathbb{P}_R^1 doesn't intersect the Zariski closures of a_1, \dots, a_r . Let $s : \text{Gal}(K)^{(p')} \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$ be the section induced by \bar{o} . Let $\alpha_1, \dots, \alpha_r$ be the images in $\pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\})$ of a bouquet of loops in $\pi_1^{\text{top}}((\mathbb{P}_{\mathbb{C}}^1)^{\text{an}} \setminus \{a_1, \dots, a_r\}, \bar{o})$ around a_1, \dots, a_r . Let G be a finite group, and let $X_K \rightarrow \mathbb{P}_K^1$ be a G -Galois branched cover ramified over a_1, \dots, a_r with branch cycle description (g_1, \dots, g_r) . Since $X_K \rightarrow \mathbb{P}_K^1$ is defined over K , it follows that there exists an $h \in G$ such that ${}^{s(\delta)}g_i = {}^h g_i$ for $i = 1, \dots, r$. Let X_R be the normalization of \mathbb{P}_R^1 in $\kappa(X_K)$.

Theorem 10.2. *In the situation above, the element h generates the inertia of some divisor above the vertical divisor in the cover $X_R \rightarrow \mathbb{P}_R^1$.*

Proof. Let P be the underlying K -rational point of \bar{o} . There exists an isomorphism between the strict henselization of the stalk of \mathbb{P}_R^1 at P and $R[[x]]^{\text{alg}}$. This induces a morphism $\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}]) \rightarrow \mathbb{P}_K^1$. Note that $\pi'_1(\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}])) \cong \hat{\mathbb{Z}}^{(p')}$. Let Δ denote the topological generator of $\pi'_1(\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}]))$ given by $t^{\frac{1}{m}} \mapsto e^{\frac{2\pi\sqrt{-1}}{m}} t^{\frac{1}{m}}$ for every m coprime to p . If H is a finite prime-to- p group, then the image of Δ in any a map $\pi'_1(\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}])) \twoheadrightarrow H$ is the generator of a divisor above (t) in the corresponding H -Galois branched cover of $\text{Spec}(R[[x]]^{\text{alg}})$. It is easy to see that the map $\rho : \pi'_1(\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}])) \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o}) \twoheadrightarrow G$ corresponds to a connected component of the cover $\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}]) \times_{\mathbb{P}_K^1} X_K \rightarrow \text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}])$, and that the image of any divisor above (t) in the induced cover of $\text{Spec}(R[[x]]^{\text{alg}})$ maps to a divisor above (t) in X_R . Since $\Delta \mapsto s(\delta)$ in the homomorphism $\pi'_1(\text{Spec}(R[[x]]^{\text{alg}}[\frac{1}{t}])) \rightarrow \pi'_1(\mathbb{P}_K^1 \setminus \{a_1, \dots, a_r\}, \bar{o})$, it follows that $\rho(\Delta) = h$ generates the inertia of some divisor above (t) in X_R . \square

REFERENCES

- [1] Artin, Michael. "Algebraization of formal moduli: I," Global Analysis: Papers in Honor of K. Kodaira, Princeton Univ. Press (1969), 21-71.
- [2] Beckmann, Sybilla. "Ramified primes in the field of moduli of branched coverings of curves," J. Algebra 125 (1989), 236-255.
- [3] Birman, Joan. "Braids, Links, and Mapping Class Groups," Annals of Mathematics Studies, no. 82 (1974).
- [4] Coombes, Kevin; Harbater, David. "Hurwitz families and arithmetic Galois groups," Duke Math J., 52 (1985), 821-839.
- [5] Farb, Benson; Margalit, Dan. "A Primer on Mapping Class Groups," Princeton Mathematical Series, 49 (2012).
- [6] Flon, Stéphane. "Ramification dans le corps des modules," Ann. Inst. Fourier (Grenoble) 54 (2004), no. 2, 253-293.
- [7] Fried, Michael; Jarden, Moshe. "Field Arithmetic," third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin (2008).
- [8] Gerritzen, Lothar; Herrlich, Frank; van der Put, Marius. "Stable n -pointed of projective lines," Nederl. Akad. Wetensch. Indag. Math. 50 (1988), no. 2, 131-163.
- [9] Grothendieck, Alexander. "Séminaire de Géométrie Algébrique," mimeographed notes (1960-61), I.H.E.S., Paris, no. 1.
- [10] Grothendieck, Alexander; Murre, Jacob. "The Tame Fundamental Group of a Formal Neighborhood of a Divisor with Normal Crossings on a Scheme," Lecture Notes in Mathematics, Vol. 208. Springer-Verlag, Berlin-New York, 1971.
- [11] Obus, Andrew. "Fields of moduli of three-point G -covers with cyclic p -Sylow, I," Algebra Number Theory, Vol. 6 (2012), no. 5, 833-883.
- [12] Obus, Andrew. "Fields of moduli of three-point G -covers with cyclic p -Sylow, II," 2010 preprint, available at arXiv:1001.3723.
- [13] Saïdi, Mohamed. "Revêtement modérés et groupe fondamental de graphe de groupes," Compositio Math. 107 (1997), no. 3, 319-338.
- [14] Stix, Jakob. "A general Seifert-Van Kampen theorem for algebraic fundamental groups," Publications of RIMS 42 (2006), no. 3, 763-786.
- [15] Szamuely, Tamás. "Galois Groups and Fundamental Groups," Cambridge Studies in Advanced Mathematics, 117. Cambridge University Press, Cambridge, 2009.
- [16] Wewers, Stefan. "Construction of Hurwitz Spaces," Ph.D. Thesis (1998), Universität Duisburg-Essen.
- [17] Wewers, Stefan. "Three point covers with bad reduction," J. Amer. Math. Soc. 16 (2003), 991-1032.

Current author information:

Hilaf Hasson: Department of Mathematics, Pennsylvania State University, State College, PA 16802, USA

email: hilafhasson@gmail.com